

REMARKS

The Applicants do not believe that examination of this response will result in the introduction of new matter into the present application for invention. Therefore, the Applicants, respectfully, request that this response be entered in and that the claims to the present application, kindly, be reconsidered.

The Final Office Action dated March 24, 2006 has been received and considered by the Applicants. Claims 1-7 and 10-22 are pending in the present application for invention. Claims 1-7 and 10-22 are rejected by the March 24, 2006 Final Office Action.

The Final Office Action rejects Claim 10-12 and 21-22 under the provisions of 35 U.S.C. §112, second paragraph, for failing to set forth the subject matter that the Applicants regard as the invention. The Examiner states that the term within rejected claim 21 that its output is 1/s biased by interpreting emitted symbols "0"... 's-n-1' as 'unencrypted' and 's-n'...'s-1' as 'encrypted' is not understood. The Applicants, respectfully, remind the Examiner that the Applicants have the right to be their own lexicographer and that the definition supplied by the specification to the present invention is to be used for interpretation of the same term as used in the claims.

The MPEP at §2111.01 states in Part III that Applicants may be their own Lexicographer. "An applicant is entitled to be his or her own lexicographer and may rebut the presumption that claim terms are to be given their ordinary and customary meaning by clearly setting forth a definition of the term that is different from its ordinary and customary meaning(s)." *In re Paulsen*, 30 F.3d 1475, 1480, 31 USPQ2d 1671, 1674 (Fed. Cir. 1994). "Where an explicit definition is provided by the applicant for a term, that definition will control interpretation of the term as it is used in the claim." *Toro Co. v. White Consolidated Industries Inc.*, 199 F.3d 1295, 1301, 53 USPQ2d 1065, 1069 (Fed. Cir. 1999).

The embodiment of the invention wherein the linear feedback shift register is over Galois Field GF(s), and its output is 1/s biased by interpreting emitted symbols "0"... 's-n-1' as 'unencrypted' and 's-n'...'s-1' as 'encrypted' is described in the specification of the present invention on page 5, lines 6-21. Specifically, it is stated on page 5, lines 13-15 "to create a biased pseudo-random sequence with bias 1/s (i.e. out of every s packs, s-1 are unencrypted and 1 is encrypted), with s prime, the polynomial should be chosen

over $GF(s)$ ". Therefore, the foregoing clearly states that out of every s blocks, 1 is encrypted. It is further stated on page 5, lines 15-17 that the "output of the LFSR is then a random sequence of elements 1_i of $GF(s)$: 0, 1, 2, ..., $s-1$. If every 1_i is replaced by 'u' if $1_i \geq 1$, and by 'c' if $1_i = 0$, otherwise, a recipe to encrypt the packs with the required bias is obtained." It is then clearly, and unequivocally stated on page 5, lines 17-21 that the foregoing "principle can be generalized to pseudo-random sequences with bias $1/s$, where s is not just prime, but the power of a prime. In an embodiment the linear feedback shift register is over Galois field $GF(s)$ and its output is biased by interpreting emitted symbols '0' ... 's-n-1' as 'unencrypted' and 's-n' ... 's-1' as 'encrypted'." Accordingly, the terminology that the Examiner asserts is not understood is clearly defined by the specification. The clear definition must be applied for claim interpretation. The statement by the Examiner that for the purpose of examination the phrase is treated as though bits other 0's represent encryption has no basis in the rejected claims or within the clear definition that is supplied by the specification. The term its output is $1/s$ biased by interpreting emitted symbols "0"... 's-n-1' as 'unencrypted' and 's-n'...'s-1' is defined to be a generalization of the above described operation. This is the definition that is supplied by the Applicants, the Applicants have the right to be their own lexicographer, and that definition must be applied during interpretation of that term within the claims. Therefore, this rejection is traversed.

Regarding Claims 22 and 10-12, the Examiner states that it is not clear how to embed a signal by selecting a key. The Applicants draw the Examiner's attention to the specification on page 5, lines 22-24 wherein it is stated that "the second signal is embedded in the first signal by selecting a key for at least partly encrypting the information from one of at least two groups of keys." The Applicants assert that this recitation within Claim 22 is abundantly clear. The selected key is used for at least partly encrypting information. Therefore, this rejection is traversed.

The Final Office Action rejects Claims 1-3 and 13-20 under the provisions of 35 U.S.C. §102(a) as being anticipated by an article within C.B.S. Proceedings of the IEEE, Volume: 87, Issue: 7, July 1999, pp. 1267-1276), entitled "Copy protection for DVD video", authored by Bloom, J.A.; Cox, I.J.; Kalker, T.; Linnartz, J.-P.M.G.; Miller, M.L.; Traw, (hereinafter referred to as Bloom et al.).

Bloom et al. is directed to copy protection using watermarking and teach watermarking as a technique for hiding information directly in video on page 1269, col. 1. Bloom et al. further teach employing a wobble within a disc that can be detected upon insertion of a disc into a compliant drive to read the payload. Bloom et al. teach that a wobble can implement a ticket to control playback (see page 1275 col. 1). It is the basic premise of Bloom et al. that only if the transformed wobble bits match the additional watermark payload then playback allowed (see page 1275 col. 1).

The Examiner's position is that Bloom et al. in teaching that only if the transformed wobble bits match the additional watermark payload then playback is allowed is tantamount to disclosure of the subject matter for "a second signal logically embedded in the first signal indicating that a physical mark is used for storing at least part of the information on the information carrier, and on the second signal being used for refusing play back of the information read from the information carrier if the second signal but no physical mark is detected" as defined by the rejected claims. The Applicants can not concur with these allegations contained within the Final Office Action. There is no disclosure or suggestion within Bloom et al. for any action to be taken if the wobble is not detected. The Applicants, respectfully, request that the Examiner indicate any portion of Bloom et al. that discloses or suggests any action that is taken or prevented from being taken upon the detection of the absence of a wobble groove (physical mark).

The Examiner clearly reads the wobble groove within Bloom et al. as being the physical mark as defined by the rejected claims. The rejection attempts to employ actions that are performed by Bloom et al. upon detection of the wobble groove with the clear recitation within the rejected claims of actions that occur if the physical mark (the wobble groove) is not detected. The rejection contradicts itself. The Applicants, respectfully, point out that it is impossible for Bloom et al. to anticipate the rejected claims because the subject matter for the second signal but no physical mark is detected is not disclosed or suggested by Bloom et al. Therefore, this rejection is respectfully traversed.

The Final Office Action rejects Claims 4-7, 10-11 and 21-22 under the provisions of 35 U.S.C. §103(a) as being unpatentable over International Publ. No. WO

99/11020 (Glogau et al.) in view Bloom et al.) and further in view of U.S. Patent No. 5,940,134 issued to Wirtz (hereinafter referred to as Wirtz).

The Examiner states that Glogau et al. teach the first signal in which a second signal is logically embedded. The Examiner further states that Glogau et al. do not teach a physical mark used for storing at least part of the information on the information carrier and for refusing playback if the second signal bit no physical mark has been detected.

The Examiner asserts that Bloom et al. teach that a physical mark is used for storing information on the information carrier and refusing playback if the second signal but no physical mark has been detected. The construction made by the Examiner in the rejection is an impossible construction. The rejected claims define subject matter for "if a second signal but no physical mark is detected". The rejected claims can not be read so broadly to as to encompass the wobble groove as the first signal because this would not be possible to in view of the wording of the rejected claims. The first signal can not be read as being the physical mark because if there is no physical mark, as defined by the rejected claims, the first signal and the second signal can still exist. Accordingly, the rejection does not address all the elements defined by the rejected claims.

There is no disclosure or suggestion within Bloom et al. for a second signal that is logically embedded in the first signal indicating that a physical mark is used for storing at least part of the information on the information carrier. Additionally, there is no disclosure or suggestion within Bloom et al. for the second signal to contain a single bit trigger that may be used for refusing play back of the information read from the information carrier if a second signal but no physical mark has been detected.

The Examiner states that Wirtz in the Abstract and col. 2, lines 43-47 teaches that the first signal/physical mark in which a second signal is logically embedded, and which could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark were detected. The Applicants, respectfully point out that Wirtz teaches to check the embedded watermark against the disc's wobble key and reproduce the signal if the authenticity of the signal is acknowledged. The Examiner appears to be reading the first signal and the physical

mark as being one in the same with the second signal being the disc's wobble key taught by Wirtz being embedded within the within the wobble groove (the physical mark). This construction is impossible because the rejected claims define subject matter for "if a second signal but no physical mark are detected". Therefore, the rejected claims can not be read so broadly that the first signal encompasses the wobble groove because this is not possible in view of the wording of the rejected claims. The first signal can not be the physical mark. Accordingly, the rejection does not address all the elements defined by the rejected claims.

This rejection does not make a *prima facie* case of obviousness.

Therefore, this rejection is respectfully traversed.

Regarding the above discussed rejection of claims 4-7 under the provisions of 35 U.S.C. §103(a) as being obvious over Glogau et al. in view Bloom et al. and further in view Wirtz. The Examiner states that Glogau et al. in view Bloom et al. the first signal do not explicitly teach the linear feedback shift register (LFSR) being over a Galois Field. The Examiner then asserts that the choice of a minimal and irreducible polynomial function would have been obvious to a person of ordinary skill within the art. The subject matter for the linear feedback shift register (LFSR) being over a Galois Field as been defined by the claims to the present invention since this case was originally filed.

The Examiner states that Bloom et al. that the second signal is embedded in the first signal by encoding a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence is generated based upon a linear feedback shift register. The Applicants do not agree with this allegation. There is no disclosure or suggestion within Bloom et al. for the encryption sequence to be generated based upon the output of a linear feedback shift register.

The Examiner then states that Glogau et al. teach the second signal being embedded in the first signal by encoding in a pseudo-random noise pattern in encrypted and unencrypted packs of the first signal, wherein the encryption sequence is generated based on a linear feedback register on page 2, lines 14-17. The Applicants, respectfully point out Glogau et al. on page 2, lines 14-17 simply states that the encryption sequence is substantially random, that can be generated based on a linear feedback register and that the encryption sequence is embedded into the carrier signal by performing an exclusive-

OR of the encryption sequence with a portion of the carrier signal.

Rejected Claim 4 defines the apparatus of claim 1, wherein the single bit trigger is contained within a message containing encrypted and unencrypted packs. The rejection does not address this feature and, therefore, does not make a *prima facie* case of obviousness. Furthermore, as previously discussed, the subject matter of refusing play back of the information read from the information carrier if the second signal but no physical mark has been detected is not found within any of the cited references.

Rejected Claim 5 defines the apparatus of claim 1, wherein the second signal is embedded in the first signal by encoding it in a predetermined pattern of encrypted and unencrypted packs of the first signal. The rejection does not address this feature and, therefore, does not make a *prima facie* case of obviousness. Furthermore, as previously discussed, the subject matter of refusing play back of the information read from the information carrier if the second signal but no physical mark has been detected is not found within any of the cited references.

Claims 6 and 7 depend from the above discussed claims and are believed to be allowable for that reason.

Regarding Claim 21, the XOR function taught by Glogau et al. does not disclose or suggest the linear feedback shift register is over Galois Field GF(s), and its output is 1/s biased by interpreting emitted symbols "0"... 's-n-1' as 'unencrypted' and 's-n'...'s-1' as 'encrypted' for the reason previously discussed in the response to the rejection under Bloom et al.

Regarding Claim 22, the Final Office Action takes Official Notice that it is old and well known to protect data signals using by encrypting the data signals using encryption keys. The Applicants, respectfully, assert that it is not well known to embed a second signal in the first signal by selecting a key for at least partly encrypting the information from one of at least two groups of keys as defined by Claim 22. The Applicants request that the Examiner produce prior art references illustrating that it is well known to embed a second signal in the first signal by selecting a key for at least partly encrypting the information from one of at least two groups of keys as defined by Claim 22. Therefore, this rejection is traversed.

The Final Office Action rejects Claims 10, 11 under the provisions of 35 U.S.C. §103(a) as being unpatentable over Glogau et al. in view Bloom et al. and further in view of Wirtz. The Examiner states that the combination of Glogau et al. with Bloom et al. and Wirtz

does not disclose or suggest selecting the key from at least one of two groups of keys. The Examiner takes Official Notice that is old and well known to have more than one key available in the system. The Examiner alleges that Taguchi et al. (U.S. Patent No. 5,915,025) teach multiple groups with multiple keys. The Applicants assert that Taguchi et al. do not disclose or suggest an apparatus as defined by claim 10, wherein a key detection algorithm is used to select the key and to decode from which group of keys said key has been selected an apparatus as defined by claim 11, wherein the decoding algorithm comprises an examining process of the outcome of projecting an n-bit key onto a set of fixed n-bit numbers. Therefore this rejection is traversed.

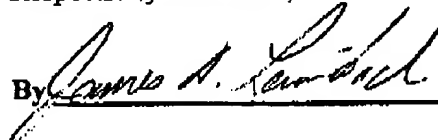
The Final Office Action rejects Claim 12 under the provisions of 35 U.S.C. §103(a) as being unpatentable over Glogau et al. in view Bloom et al. and further in view of Wirtz. The Examiner states that the combination of Glogau et al. with Bloom et al. and Wirtz does not disclose or suggest that the examining process takes the form of going down a binary tree, where going left is caused by projection-value 0 and right by projection in value non-zero. The Examiner takes Official Notice that is old and well known to use a binary search for more efficient searching and also that in a binary tree going one direction is caused by one projection value and another direction caused by another projection value. The Examiner cites "Algorithms", second edition, 1998, ISBN: 0201066734, pg. 198 by Robert Sedgewick (hereinafter Sedgewick) for support of this allegation. The Applicants assert that Sedgewick does not disclose or suggest an examining process that takes the form of going down a binary tree, where said going left is caused by projection-value 0 and right by projection in value non-zero as defined by claim 12. Therefore, this rejection is traversed.

Applicant is not aware of any additional patents, publications, or other information not previously submitted to the Patent and Trademark Office which would be required under 37 C.F.R. 1.99.

In view of the foregoing amendment and remarks, the Applicant believes that the present application is in condition for allowance, with such allowance being, respectfully, requested.

The Commissioner is hereby authorized to credit any overpayment or charge any fee (except the issue fee) including fee for any required extension of time, to Account No. 50-3745.

Respectfully submitted,

By 

James D. Leimbach
Patent Attorney Reg. No. 34,374

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence
is being transmitted on this date via
facsimile transmission to (571) 273-8300 AND addressed to:
Mail Stop: AF
COMMISSIONER OF PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Date of Transmission: May 8, 2006

(Signature) 
By: James D. Leimbach